UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,001	02/01/2002	Yaakov (Jordan) Levy	86120	2537

7590 07/13/2005

Gerald T. Shekleton, Esq.
Welsh & Katz, Ltd.
22nd Floor
120 S. Riverside Plaza
Chicago, IL 60606

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 07/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/062,001	LEVY, YAAKOV (JORDAN)	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/7/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 2/1/2002.

DETAILED ACTION

Claims 1-16 have been examined.

Title

The title of the invention is acceptable.

Priority

This application claims priority to ISRAEL 142962, filed on 5/3/2001.

Therefore, the effective filing date for the subject matter defined in the pending claims in this application is 5/3/2001.

Information Disclosure Statement

The information disclosure statement(s) (IDS) submitted on 5/7/2002 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statements.

Drawings

The drawings filed on 2/1/2002 are acceptable for examination proceedings.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure is objected to because:

Line 1 recites "is described" which can be implied and must therefore be removed.

Lines 5-6 recite "Related methods and apparatus are also described" which can be implied and must be removed.

The abstract is objected to for failing to meet the length requirement of 50 words.

Correction is required. See MPEP § 608.01(b).

The disclosure is objected to because of the following informalities:

Throughout the specification and beginning on line 16 of page 7, the acronym "SIG" is used but is never defined. As such, it would be unclear to the reader what "SIG" is meant to represent.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-15 are directed towards a method for digitally signing a message, but the claims fail to indicate any subject matter that is statutory. All of the method steps could be performed by a person using a pen and paper. As such, these claims are non-statutory and are therefore rejected under 35 USC 101.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1 and 16 recite the limitation "SIG" which is an acronym that has not been defined. Therefore, the ordinary person skilled in the art would be unable to determine what a "SIG" is and therefore would be unable to determine the scope of the claim. Therefore, claims 1 and 16 are rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

Claims 2-15 are rejected by virtue of their dependency to claim 1.

Claim 1 recites the limitation "assigning SIG" in Line 8. There is insufficient antecedent basis for this limitation in the claim.

Claim 1 recites the limitation "(x,y)" in Line 9. There is insufficient antecedent basis for this limitation in the claim.

Claim 2 recites the limitation "(x,y,z)" in Line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "α" in Line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "β" in Line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "k" in Line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "γ" in Line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "n" in Line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "R" in Line 6. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "T" in Line 7. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "U" in Line 8. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "W" in Line 8. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "D" in Line 10. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "A" in Line 11. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "B" in Line 12. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "C" in Line 15. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 recites the limitation "gcd()" in Line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites the limitation "α" in Line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites the limitation "β" in Line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites the limitation "k" in Line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites the limitation "γ" in Line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites the limitation "n" in Line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites the limitation "T" in Line 6. There is insufficient antecedent basis for this limitation in the claim.

Any claim not specifically mentioned above is rejected by virtue of its dependency to a previously rejected claim.

Claims 11-15 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: All steps pertaining to α and all steps pertaining to β. Although the examiner understands, from the specification and the disclosed steps therein, that when $\alpha = 0$ and $\beta = 1$ the equations required by the method become simplified, it would be unclear to the ordinary person skilled in the art how α and β are used in the method. It appears to

the examiner that the equations still contain α and β, and they effectively make the equations simpler to solve. In the recitations of the current claim 11, α and β appear to have no purpose, which is misleading since this is not the case. Claims 12-15 are rejected by virtue of their dependency to claim 11.

Claim 16 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are:

i. the structure of the solver.

ii. the structure of the signature assignor.

iii. the relationship between the solver and the signature assignor.

These structures and relationships are essential to the understanding of how the elements of the claim together make up a message signer. As such, claim 16 is rejected under 35 USC 112 2nd paragraph.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 11, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ong et al. ("An Efficient Signature Scheme Based on Quadratic Equations") hereinafter referred to as Ong, and further in view of Okamoto et al. ("An Efficient Digital Signature Scheme Based on an Elliptical Curve Over the Ring Z_N") hereinafter referred to as Okamoto.

Regarding claims 1 and 16, Ong disclosed a method for digitally signing a message (See Ong Abstract Lines 7-18), the method comprising:

providing a modulus N (See Ong Equation 1 'n');

providing a number V in the ring Z_N (See Ong Equation 2 'k'), wherein for another number S in the ring Z_N, $V \cdot S^2 = 1$ in Z_N (See Ong Equation 2 'u'),

solving an equation in Z_N to provide x and y (See Ong Equation 1 's_1' and 's_2'); and

assigning SIG as the signature of the message, wherein SIG comprises (x,y,z) (See Ong Equation 8 and following paragraph), however, Ong failed to disclose providing a message digest to sign instead of the message itself, or solving the equation:

$(M_x + 1)^2 - V \cdot y^2 = 4(M_Z + z)$ for x, y, and z.

It was well known in the art at the time of invention to provide a message digest for signing in place of the message itself in order to reduce the computation time required to produce the signature. It therefore would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was known in the art in the signature scheme of Ong by signing a message digest of the message in place of the message. This would have been obvious because the ordinary person skilled in the art would have been motivated to decrease the computation time required to perform the signing.

Okamoto teaches a signature scheme based on Elliptic curve over Z_N involving a multiple variable signature (See Okamoto Section 5.4.2) wherein the signing is performed on the message digest (m_x, m_y) of the message (See Okamoto Page 62 Lines 13-15). Okamoto further teaches that a signature can be composed of multiple variables and the signature is formed by solving a one way multivariable formula for the variables (See Okamoto Section 5.3 – 5.3.1).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Okamoto in the signature generation of Ong by solving a one way multivariable equation in order to determine the signature. This would have been obvious because the ordinary person skilled in the art would have been motivated to increase the complexity of the signature scheme in order to increase the security of the scheme. Furthermore, the specific claimed equation is simply one of many one way multivariable equations and therefore would have been an obvious variation as well.

Regarding claim 2 the combination of Ong and Okamoto disclosed a multivariable signature (See Okamoto Section 5.3.1).

Regarding claims 3 and 11, it would have been obvious to the ordinary person skilled in the art at the time of invention to perform the steps of these claims by using well known mathematical strategies for solving equations. This would have been obvious because the ordinary person skilled in the art would have been motivated to use mathematics in order to solve the equation for the variables.

Conclusion

Claims 1-16 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Ong et al. ("Efficient Signature Schemes Based on Polynomial Equations") disclosed a signature scheme which took a message M1 and M2 and produced a multiple component signature.

b. Maurer (US Patent Number 5,146,500) disclosed a signature scheme based on elliptical curve over rings.

c. Orton (US Patent Number 5,297,206) disclosed a signature scheme involving a multiple component signature.

d. Galbraith ("Elliptic Curve Paillier Schemes") disclosed encryption schemes over elliptic curves.

e. Paillier ("Trapdooring Discrete Logarithms on Elliptic Curves over Rings") disclosed encryption schemes over elliptic curves over rings.

f. Biehl et al. ("A Signature Scheme Based on the Intractability of Computing Roots") disclosed a signature scheme which produced a signature with three components.

g. Koyama et al. ("New Public-Key Schemes Based on Elliptic Curves over the Ring Z_N") disclosed a signature scheme which produced a multiple component signature.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
7/8/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100